AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated below. The language being added is underlined ("__") and the language being deleted contains a strikethrough ("—").

LISTING OF CLAIMS

1. (Currently Amended) A method for generating pseudo-random numbers, comprising the steps of:

loading a current seed value S_j from a non-volatile storage;

loading a value, E, representative of environmental randomness;

loading a value, C, representative of configuration data;

reading a first fixed value, A;

reading a second fixed value, B;

generating a new seed value, S_{j+1}, in accordance with the following equation:

$S_{j+1}=f(S_j; A; C; E)$, wherein f represents a selected encryption algorithm, ~~and B is a second constant,~~ and wherein S_j is concatenated with A, which is concatenated with C which is concatenated with E;

writing the new seed value S_{j+1} to the non-volatile storage;

generating a key, K, in accordance with the following equation:

$K=f(S_j; B; C; E)$, ~~wherein B is a second constant;~~ and

generating a pseudo-random number output, P_n, in accordance with the following equation:

$P_n=f_{3DES}(K, P_{n-1})$, where f_{3DES} represents the operation of triple DES encryption hardware, and P_{n-1} is the previously generated pseudo-random

number.

2. (Original) The method of claim 1, wherein the function f comprises the FIPS 180 secure hash standard algorithm (SHA).

3. (Original) The method of claim 1, wherein the value E includes at least 80 bits of entropy.

4. (Original) The method of claim 1, wherein the seed S_j is 160 bits in length.

5. (Original) The method of claim 1, wherein the seed S_j is 256 bits in length.

6. (Original) The method of claim 1, wherein the seed S_j is 512 bits in length.

7. (Original) The method of claim 1, wherein an initial value of P_0 is 0.

8. (Original) The method of claim 1, further comprising the steps of loading values for the first and second constants A and B from a protected ROM address.

9. (Currently Amended) The method of claim 8, wherein the first and second fixed values~~constants~~ A and B further incorporate a copyright notice embedded therein.

10. (Original) The method of claim 1, wherein the f_{3DES} hardware is operated in output feedback mode.

11. (Original) The method of claim 1, wherein the f_{3DES} hardware is operated in dual counter mode.

12. (Currently Amended) A computer-readable medium having a program stored thereon ~~incorporating one or more instructions~~ for generating pseudo-random numbers, the program~~instructions~~ comprising:

one or more instructions for loading a current seed value S_j from a non-volatile storage;

one or more instructions for loading a value, E, representative of environmental randomness;

one or more instructions for loading a value, C, representative of configuration data;

one or more instructions for loading a first fixed value, A;

one or more instructions for loading a second fixed value, B;

one or more instructions for generating a new seed value, S_{j+1}, in accordance with the following equation:

$S_{j+1}=f(S_j; A; C; E)$, wherein f represents a selected encryption algorithm, ~~and B is a second constant,~~ and wherein S_j is concatenated with A, which is concatenated with C which is concatenated with E;

one or more instructions for writing the new seed value S_{j+1} to the non-volatile storage;

one or more instructions for generating a key, K, in accordance with the following equation:

$K=f(S_j; B; C; E)$~~,wherein B is a second constant~~; and

one or more instructions for generating a pseudo-random number output, P_n, in

accordance with the following equation:

$P_n=f_{3DES}(K, P_{n-1})$,wherein f_{3DES} represents the operation

of triple DES encryption hardware, and P_{n-1} is the previously generated pseudo-random number.

13. (Original) The computer-readable medium of claim 12, wherein the function f comprises the FIPS 180 secure hash standard algorithm (SHA).

14. (Original) The computer-readable medium of claim 12, wherein the value E includes at least 80 bits of entropy.

15. (Original) The computer-readable medium of claim 12, wherein the seed S_j is 160 bits in length.

16. (Original) The computer-readable medium of claim 12, wherein the seed S_j is 256 bits in length.

17. (Original) The computer-readable medium of claim 12, wherein the seed S_j is 512 bits in length.

18. (Original) The computer-readable medium of claim 12, wherein an initial value of P_0 is 0.

19. (Currently Amended) The computer-readable medium of claim 12, further comprising one or more instructions for loading values for the first and second fixed values ~~constants~~ A and B from a protected ROM address.

20. (Currently Amended) The computer-readable medium of claim 19, wherein the first and second fixed values ~~constants~~ A and B further incorporate a copyright notice embedded therein.

21. (Original) The computer-readable medium of claim 12, wherein the f_{3DES} hardware is operated in output feedback mode.

22. (Original) The computer-readable medium of claim 12, wherein the f_{3DES} hardware is operated in dual counter mode.